

### **REMARKS**

Claims 1-4, 43-46, and 90-103 are currently pending in the present application. Claims 1-4, 43-46, and 90-103 stand rejected. Claims 1, 43, 90, and 98 have been amended. No claims have been added or cancelled. Reconsideration of the pending claims is requested in light of the present amendments and remarks.

Amendments have been made to the claims to provide a better understanding of the claims, in that the term “third” server has been changed to “second” server. This has been done because there was no specific recital of a “second” server in the claims, so Applicants felt that reference to a “third” server might be confusing. Applicants have corrected this potential confusion, and respectfully submit that the amendment was not done for purposes of patentability.

### **Rejections of Claims 1-3, 43-45, and 90 Under 35 U.S.C. § 103(a)**

The Examiner has rejected claims 1-3, 43-45, and 90 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,263,446 to Kausik et al. in view of U.S. Patent No. 6,327,578 to Linehan et al. Applicants respectfully traverse the rejection.

### **Rejection of Claim 1 and 2-4**

Applicants respectfully submit that neither Kausik nor Linehan, alone or in combination, disclose, teach, or suggest the all the elements of claim 1. Claim 1, as amended herein, is directed to a method for conducting a transaction. Among other elements, claim 1 requires issuing a challenge to a second server and forwarding the challenge from said second server to the user, wherein said challenge is passed to an intelligent token for processing said challenge, wherein said intelligent token generates a response to said challenge; receiving said response at said second server from the user based upon said challenge; and processing said response at said second server to verify the intelligent token.

U.S. Patent No. 6,263,446 to Kausik et al (Claim 1 and 2-4)

Kausik is directed to obtaining an authentication credential usable to conduct an electronic transaction. Kausik teaches that a credential server (first server) receives a request from a browser (*i.e.*, user). In response, the credential server (first server) sends a challenge *directly* to a user in the form of a shared secret that has previously been associated with the user during the set-up phase. (See Kausik, col. 4, lns. 13-17). The user provides a response to the challenge *directly* to the credential server. The credential server processes the response to determine if the user provided a correct answer to the credential server. If the user provides a correct answer to the credential server, the credential server obtains the user's wallet from the wallet database. (See Kausik, col. 4, lns. 13-18).

However, Kausik fails to teach a credential server (first server) that issues a challenge to a wallet server (second server) that forwards the challenge to the user, receiving a response to the challenge at the wallet server (second server) and processing the response to the challenge at the wallet server (second server). Instead, Kausik issues a challenge *directly* to the user, the user provides a response *directly* to the credential server, and the credential server processes the response to the challenge at the credential server. The wallet server, as disclosed by Kausik, does not process the response to the challenge to determine if the response is correct.

In addition, Kausik does not disclose, teach, or suggest assembling credentials for the transaction; providing the credentials to the user; receiving, at said second server, a second request from said user, said second request including said portion of said assembled credentials provided to said user; and validating, at said second server, said portion of said assembled credentials provided to said user with said key of said assembled credentials to provide access to a transaction service, as required by claim 1.

Instead, as stated above, Kausik teaches that the credential server (first server) receives only a *first request directly* from the user and in response sends a challenge to the user. The user provides a response to the challenge and based on the user's response, the credential server (first server) provides the wallet to the user. Indeed, no credentials or portions thereof are provided to the user after verification, as required by step [f] of claim 1. Moreover, Kausik does not disclose, teach, or suggest that the credential server (first server) or any other server (*e.g.*, second server) receives a *second request* at a *second server* wherein the second request includes a portion of the assembled credentials, and in response to the *second request*, the *second server* provides access to the transaction service.

Conversely, in the claimed invention, the wallet server (second server) acts as a proxy for the user during the transaction. With that in mind, the wallet server (second server) receives the issued challenge, forwards the issued challenge to the user, and processes the response to the challenge to verify the user's identity, and upon verification, transmits a security token (assembled credentials) to the user. In addition, the wallet server (second server) receives a second request which includes the security token (assembled credentials) from the user and validates the security token to provide access to the transaction service.

This added security, which is not disclosed, taught, or suggested by Kausik, provides the claimed invention with added confidence in the identity of the user, thereby justifying a lower discount rate for the transaction. (See Application, pg. 26, lns. 9-12).

Indeed, Applicants further submit that there is no suggestion to modify Kausik, as contended by the Examiner, to include the claimed method where a credential server issues a challenge to a wallet server (second server) that forwards the challenge to the user. Kausik is intended for the rapid deployment of credentials and in that manner, the credential server issues the

challenge directly to the user. (See. Kausik, col. 2, lns. 60-62). Conversely, the claimed invention provides added security because the credential server must issue the challenge to the wallet server that forwards the challenge to the user. Issuing a challenge to a wallet server that forwards the challenge to the user in the manner of the claimed invention would subvert the intended goal of Kausik because the speed at which the challenge is issued to the user is reduced.

U.S. Patent No. 6,327,578 to Linehan et al. (Claims 1 and 2-4)

Linehan fails to teach or disclose the invention claimed in claim 1, when combined with Kausik. Specifically, Applicants respectfully submit that Linehan does not disclose, teach, or suggest the “issuing a challenge to a second server and forwarding the challenge from said second server to the user, wherein said challenge is passed to an intelligent token for processing said challenge, wherein said intelligent token generates a response to said challenge; receiving said response at said second server from the user based upon said challenge; processing said response at said second server to verify the user,” as required by claim 1.

Linehan is directed to method, system, program and method of doing business for electronic commerce. Linehan teaches that an issuer gateway (first server) transmits a challenge to a consumer computer (user) which passes the challenge on to a smart card reader. The smart card reader signs the challenge and returns the signed challenge response to the consumer computer (user), which then transmits the signed challenge to the issuer gateway (first server). The issuer gateway (first server) verifies the signature and thus verifies the consumer identify. (See Linehan, col. 7, lns. 25-38).

However, Linehan fails to teach an issuer gateway (first server) that issues a challenge to a wallet server (second server) that forwards the challenge to the user, receiving a response to the challenge at the wallet server (second server) and processing the response to the challenge at the

wallet server (second server). Instead, in Linehan, the issuer gateway (first server) issues a challenge *directly* to the user (consumer computer), the user provides a response to the issuer gateway (first server), and the issuer gateway (first server) processes the response to the challenge at the issuer gateway (first server). In particular, Linehan also fails to disclose a second server (*i.e.*, wallet server) that processes the response to the challenge to determine if the response is correct. Instead, the issuer gateway (first server) processes the response.

Moreover, Applicants submit that the consumer computer cannot be considered to be the second server because the consumer computer does not process the response to the challenge to determine if the response is correct, as required by claim 1. As a result, Linehan fails to disclose a second server, as required by claim 1.

Conversely, as stated above, in the claimed invention the wallet server (second server) acts as a proxy for the user during the transaction. With that in mind, the wallet server receives the issued challenge from the security server (first server), forwards the issued challenge to the user, and processes the response to the challenge to verify the user's identity, and upon verification, transmits a security token (assembled credentials) to the user.

This added security, which is not disclosed, taught, suggested by Linehan, provides the claimed invention with added confidence in the identity of the user, thereby justifying a lower discount rate for the transaction. (See Application, pg. 26, lns. 9-12).

Indeed, Applicants further submit that there is no suggestion to modify Linehan to include the claimed method where a credential server issues a challenge to a wallet server that forwards the challenge to the user. Linehan is intended to significantly reduce the complexity of an electronic transaction and improve the ease of implementation of the necessary hardware and software for such electronic transactions. (See Linehan, Abstract). Conversely, the claimed invention provides

added security because the credential server must issue the challenge to the wallet server that forwards the challenge to the user. Issuing a challenge to a wallet server that forwards the challenge to the user in the manner of the claimed invention requires additional hardware and software (*i.e.*, wallet server) and subverts the intended goal of Linehan by increasing necessary hardware and software for such electronic transactions.

Neither Kausik nor Linehan teach or disclose the elements of claim 1, alone or in combination. As a result, Applicants respectfully submit that Claim 1 is patentable over Kausik and Linehan, alone or in combination. Additionally, claims 2-4 depend on claim 1, and include all of its elements. Therefore, Applicants respectfully submit that claims 2-4 are also patentable over Kausik and Linehan, alone or in combination.

Rejection of Claim 43, and 44-46

Similarly, Applicants respectfully submit that neither Kausik nor Linehan teach or disclose the elements of claim 43, alone or in combination. Claim 43, as amended herein, is directed to a method of conducting a transaction. Among other elements, claim 43 requires issuing a challenge to a second server and forwarding the challenge from said second server to the user, wherein said challenge is passed to an intelligent token for processing said challenge, wherein said intelligent token generates a response to said challenge; receiving said response at said second server from the user based upon said challenge; and processing said response at said second server to verify the user

*U.S. Patent No. 6,263,446 to Kausik et al (Claim 43 and 44-46)*

As noted with respect to claim 1, Kausik fails to teach a credential server (first server) that issues a challenge to a wallet server (second server) that forwards the challenge to the user, receiving a response to the challenge at the wallet server (second server) and processing the response to the challenge at the wallet server (second server). Instead, Kausik issues a challenge

*directly* to the user, the user provides a response *directly* to the credential server, and the credential server processes the response to the challenge at the credential server. The wallet server, as disclosed by Kausik, does not process the response to the challenge to determine if the response is correct.

In addition, as stated with respect to claim 1, Kausik does not disclose, teach, or suggest assembling credentials for the transaction; providing the credentials to the user; receiving, at said second server, a second request from said user, said second request including said portion of said assembled credentials provided to said user; and validating, at said second server, said portion of said assembled credentials provided to said user with said key of said assembled credentials to provide access to a transaction service, as required by claim 43.

Similarly, Applicants submit that there is no suggestion to modify Kausik to include the claimed step of issuing a challenge to a wallet server that forwards the challenge to user because Kausik is intended for rapidly deploying challenges to the user rather than providing additional security as described above.

*U.S. Patent No. 6,327,578 to Linehan et al. (Claims 43 and 44-46)*

Linehan fails to teach or disclose the invention claimed in claim 43, when combined with Kausik. Specifically, Linehan fails to teach an issuer gateway (first server) that issues a challenge to a wallet server (second server) that forwards the challenge to the user, receiving a response to the challenge at the wallet server (second server) and processing the response to the challenge at the wallet server (second server), as required by claim 43. In addition, Linehan fails to disclose a second server (*i.e.*, wallet server) that processes the response to the challenge to determine if the response is correct, as required by claim 43.

Moreover, Applicants submit that the consumer computer cannot be considered to be the

second server because the consumer computer does not process the response to the challenge to determine if the response is correct, as required by claim 43. As a result, Linehan fails to disclose a second server, as required by claim 1.

Similarly, Applicants submit there is no suggestion to modify Linehan to include the claimed method where a credential server issues a challenge to a wallet server that forwards the challenge to the user because Linehan is intended to significantly reduce the complexity of an electronic transaction and improve the ease of implementation of the necessary hardware and software for such electronic transactions, rather than providing additional security, as described above.

Neither Kausik nor Linehan teach or disclose the elements of claim 43, alone or in combination. As a result, Applicants respectfully submit that Claim 43 is patentable over Kausik and Linehan. Additionally, claims 44-46 depend on claim 43, and include all of its elements. Therefore, Applicants respectfully submit that claims 44-46 are also patentable over Kausik and Linehan.

#### Rejection of Claim 90, and 91-97

Similarly, Applicants respectfully submit that neither Kausik nor Linehan teach or disclose the elements of claim 90. Claim 90, as amended herein, is directed to a method of conducting a transaction. Among other elements, claim 90 requires issuing a challenge to a second server and forwarding the challenge from said second server to the user, wherein said challenge is passed to an intelligent token for processing said challenge, wherein said intelligent token generates a response to said challenge; receiving said response at said second server from the user based upon said challenge; and processing said response at said second server to verify the intelligent token.



U.S. Patent No. 6,263,446 to Kausik et al (Claim 90 and 91-97)

As noted with respect to claim 1, Kausik fails to teach a credential server (first server) that issues a challenge to a wallet server (second server) that forwards the challenge to the user, receiving a response to the challenge at the wallet server (second server) and processing the response to the challenge at the wallet server (second server). Instead, Kausik issues a challenge *directly* to the user, the user provides a response *directly* to the credential server, and the credential server processes the response to the challenge at the credential server. The wallet server, as disclosed by Kausik, does not process the response to the challenge to determine if the response is correct.

In addition, as stated with respect to claim 1, Kausik does not disclose, teach, or suggest assembling credentials for the transaction; providing the credentials to the user; receiving, at said second server, a second request from said user, said second request including said portion of said assembled credentials provided to said user; and validating, at said second server, said portion of said assembled credentials provided to said user with said key of said assembled credentials to provide access to a transaction service, as required by claim 43.

Similarly, Applicants submit that there is no suggestion to modify Kausik to include the claimed step of issuing a challenge to a wallet server that forwards the challenge to user because Kausik is intended for rapidly deploying challenges to the user rather than providing additional security as described above.

U.S. Patent No. 6,327,578 to Linehan et al. (Claims 90 and 91-97)

Linehan fails to teach or disclose the invention claimed in claim 90, when combined with Kausik. Specifically, Linehan fails to teach an issuer gateway (first server) that issues a challenge to a wallet server (second server) that forwards the challenge to the user, receiving a response to the

challenge at the wallet server (second server) and processing the response to the challenge at the wallet server (second server), as required by claim 90. In addition, Linehan fails to disclose a second server (*i.e.*, wallet server) that processes the response to the challenge to determine if the response is correct, as required by claim 90.

Moreover, Applicants submit that the consumer computer cannot be considered to be the second server because the consumer computer does not process the response to the challenge to determine if the response is correct, as required by claim 90. As a result, Linehan fails to disclose a second server, as required by claim 90.

Similarly, Applicants submit there is no suggestion to modify Linehan to include the claimed method where a credential server issues a challenge to a wallet server that forwards the challenge to the user because Linehan is intended to significantly reduce the complexity of an electronic transaction and improve the ease of implementation of the necessary hardware and software for such electronic transactions, rather than providing additional security, as described above.

Neither Kausik nor Linehan teach or disclose the elements of claim 90, alone or in combination. As a result, Applicants respectfully submit that Claim 90 is patentable over Kausik and Linehan. Additionally, claims 91-97 depend on claim 90, and include all of its elements. Therefore, Applicants respectfully submit that claims 91-97 are also patentable over Kausik and Linehan.

**Rejections of Claims 4, 46, and 91-103 Under 35 U.S.C. § 103(a)**

The Examiner has rejected claims 4, 46, and 91-103 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,263,446 to Kausik et al and U.S. Patent No. 6,327,578, and further in view of U.S. Patent No. 6,873,974 to Schutzer. Applicants respectfully traverse the

rejection.

Rejection of Claims 98-103

Applicants respectfully submit that claim 98 is patentable over Kausik and Linehan in view of Schutzer. Claim 98, as amended herein, is directed to a method for conducting an electronic purchase transaction. Among other elements, claim 98 requires issuing a challenge to a second server and forwarding the challenge from said second server to the user, wherein said challenge is passed to an intelligent token for processing said challenge, wherein said intelligent token generates a response to said challenge; receiving said response at said second server from the user based upon said challenge; and processing said response at said second server to verify the intelligent token.

U.S. Patent No. 6,263,446 to Kausik et al (Claim 98-103)

As noted with respect to claim 1, Kausik fails to teach a credential server (first server) that issues a challenge to a wallet server (second server) that forwards the challenge to the user, wherein the challenge is passed to an intelligent token for processing, receiving a response to the challenge at the wallet server (second server) and processing the response to the challenge at the wallet server (second server) to verify the intelligent token. Instead, Kausik issues a challenge *directly* to the user, the user provides a response *directly* to the credential server, and the credential server processes the response to the challenge at the credential server. The wallet server, as disclosed by Kausik, does not process the response to the challenge to determine if the response is correct.

In addition, as stated with respect to claim 1, Kausik does not disclose, teach, or suggest assembling credentials for the transaction; providing the credentials to the user; receiving, at said second server, a second request from said user, said second request including said portion of said assembled credentials provided to said user; and validating, at said second server, said portion of

said assembled credentials provided to said user with said key of said assembled credentials to provide access to a transaction service, as required by claim 98.

Similarly, Applicants submit that there is no suggestion to modify Kausik to include the claimed step of issuing a challenge to a wallet server that forwards the challenge to user because Kausik is intended for rapidly deploying challenges to the user rather than providing additional security as described above. Applicants also further submit that Schutzer fails to disclose, teach, or suggest the above-identified elements.

U.S. Patent No. 6,327,578 to Linehan et al. (Claims 98-103)

Linehan fails to teach or disclose the invention claimed in claim 98, when combined with Kausik. Specifically, Linehan fails to teach an issuer gateway (first server) that issues a challenge to a wallet server (second server) that forwards the challenge to the user, receiving a response to the challenge at the wallet server (second server) and processing the response to the challenge at the wallet server (second server), as required by claim 98. In addition, Linehan fails to disclose a second server (*i.e.*, wallet server) that processes the response to the challenge to determine if the response is correct, as required by claim 98.

Moreover, Applicants submit that the consumer computer cannot be considered to be the second server because the consumer computer does not process the response to the challenge to determine if the response is correct, as required by claim 98. As a result, Linehan fails to disclose a second server, as required by claim 98.

Similarly, Applicants submit there is no suggestion to modify Linehan to include the claimed method where a credential server issues a challenge to a wallet server that forwards the challenge to the user because Linehan is intended to significantly reduce the complexity of an electronic transaction and improve the ease of implementation of the necessary hardware and

software for such electronic transactions, rather than providing additional security, as described above. Applicants also further submit that Schutzer fails to disclose, teach, or suggest the above-identified elements.

As a result, Applicants respectfully submit that Claim 98 is patentable over Kausik and Linehan in view of Schutzer. Additionally, claims 99-103 depend on claim 98, and include all of its elements. Therefore, Applicants respectfully submit that claims 99-103 are also patentable over Kausik and Linehan in view of Schutzer.

Rejection of Claims 4, 46, and 91-97

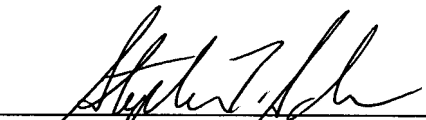
The Examiner has also rejected claims 4, 46, and 91-97 as unpatentable over Kausik and Linehan in view of Schutzer. Claims 4, 46, and 91-97 depend on claims 1, 43, and 90, respectively, and include all the elements of their respective independent claims. Therefore, Applicants respectfully submit that these claims are also patentable over Kausik and Linehan in view of Schutzer.

**CONCLUSION**

In view of the foregoing remarks and amendments, Applicants respectfully submit that all of the claims in the Application are in allowable form and that the Application is now in condition for allowance. If, however, any outstanding issues remain, Applicants urge the Examiner to telephone Applicants' attorney so that the same may be resolved and the Application expedited to issue. Applicants respectfully request the Examiner to indicate all claims as allowable and to pass the Application to issue.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP



Stephen T. Scherrer  
Registration No. 45,080

227 West Monroe Street  
Chicago, IL 60606-5096  
Phone: 312.372.2000  
Facsimile: 312.984.7700  
**Date: May 23, 2007**

**Please recognize our Customer No. 1923 as our  
correspondence address.**

CHI99 4816808-1.037355.0037